REMARKS

Claims 1-31 are currently pending in the application of which claims 1, 16, 20, 26 and 27 are independent. Claims 1, 16, 26 and 27 have been amended. No new matter has been added.

Claim Rejections Pursuant to 35 U.S.C. §101

Applicants have amended independent claims 1, 16, and 26 to explicitly cite that the user profile is being stored on an electronic device. Claim 27, upon which claims 28-31 are dependent, previously cited the limitation that the profile was held on a preference management server and therefore has not been amended. The claimed use of the user profile on the electronic device/preference management server provides the useful result of a new type of mechanism for enabling access to the user profile information. Accordingly, Applicants request the withdrawal of all of the 35 U.S.C. §101 rejections.

Claim Rejections Pursuant to 35 U.S.C. §112

Claims 1, 16, 27 and 29 were rejected as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention. More particularly, the Examiner objected to the use of the term "non-user party". Applicants have amended claims 1, 16, 27 and 29 to clarify that the "non-user party" is "an entity other than the user about which the user-profile holds information." Accordingly, Applicants request the withdrawal of the 35 U.S.C. §112 rejections.

Claim Rejections Pursuant to 35 U.S.C. §102(e)

Claims 1-31 were rejected under 35 U.S.C. §102(e) as being anticipated by Cook (United States Patent No.: 6,697,806, hereafter "Cook"). For the reasons set forth below, Applicants respectfully traverse the rejections.

Summary of the Claimed Invention

The claimed invention provides a user profile infrastructure where user profiles are accessible via a central location. The user profiles may contain information that is accessible by multiple service providers. The data in a user profile may be dispersed over multiple databases or other storage locations. Service providers that are authorized may request and retrieve the information via the infrastructure without the user getting involved. As there is only a single user profile per user, changes need only to be made via the user profile infrastructure to ensure that the user profile is kept current. A user profile may be modified by the user or authorized service providers. The user may have complete control over the user profile and may specify the information to be included in the user profile. The user may also have control over the permissions that specify what clients have permission to access information in the user profile. The permissions may specify the type of access that is provided to each client. Permissions may be specified not only for user profiles as a whole but also for individual fields within user profiles.

Summary of Cook

Cook discusses an access communication system which provides access between a user system and a plurality of communication networks. The plurality of communication networks provides services to a user in the user system. The access communication system includes a local database system and an access server connected to the user system and the plurality of communication networks. The local database system includes a user profile system which is used to determine whether the user is allowed access to the local database system.

Argument

Cook fails to disclose all of the elements of Applicants independent claims 1, 16, 20, 26 and 27. Accordingly, Applicants request the removal of the rejections directed to claims 1-31.

As noted above, Applicants claimed invention provides a user profile infrastructure where user profiles are accessible via a central location. Service providers that are authorized may request and retrieve the information via the user profile infrastructure without the user getting involved. Applicants independent claims 1, 16, 20, 26 and 27 all include this ability. Thus, Applicants independent claim 1 includes the claim element of "receiving a request from a non-user party to reference the selected subdivision [of the user profile], the non-user party being an entity other than the user about which the user-profile holds information [emphasis added]." Similarly, claim 16 includes the claim element "transmitting the authorized information to a non-user party in said selected one of the groups in response to a request from the non-user party." Likewise, claim 20 includes the claim element of "setting permissions relative to a given service provider so as to prevent access to at least one selected field and grant access in to at least one given field in the user profile so as to support an anonymous transaction between the given service provider and the user ."

Claim 26 includes the claim element of providing a protocol that enables the getting and setting of permission access permissions that specify permissions for the access permissions (i.e. who gets to set the access permissions). Also, claim 27 includes the step of "receiving a request for information from a non-user party, said request referencing a set of permissions required for access to the user profile."

The Examiner-cited reference Cook discusses an access communication system (providing an interface between the user network and the service networks, col. 8, lines 65-66) in which a "user profile is stored in the access network and controls user access to services" (col. 10, lines 25-26). The network user access profile includes 'access information' which is defined as "any information or data related to providing the user access to the network architecture" (col. 10, lines 33-35). Network user access profiles are consulted in response to a request by the user to access services. "When a user requests access to services, the access network 520 processes the user access profile for the user" col. 9, lines 29-30)[emphasis added]. This represents a significant difference from the claimed invention where a non-user party requests access to the user profile.

The Examiner cited various figure numbers as corresponding to Applicants claim elements. A closer examination however indicates that the components corresponding to the cited numbers fail to disclose all of Applicants claim elements. For example, the Examiner cited figure numbers (1302, 1312, 1316 and 1322) in Figure 13 as corresponding to Applicants'-claim 1 step of "establishing a first set of permissions for the user profile, wherein said first set of permissions specifies who may access the user profile". Figure 13 is directed to a discussion of access network user binding and has a sub-heading of "User Access Profile Mobility" (col. 14, line 53). The focus of the discussion is explained in the first sentence, "Users may access their user access profile from any network device connected to the network architecture," (col. 14, lines 54-55). In other words, the figure discusses allowing the <u>user</u> to access the profile from different devices. The figure does not discuss establishing permissions setting forth who may access the user profile, it is always the same user, albeit on different devices. Thus step 1302 determines whether the user profile is on a local database, step 1312 and 1316 determine whether a request from the user is a retrieve or release request respectively, and step 1322 determines whether the request from the user is an update request (see col. 15, lines 4-61 inclusive). The Examiner's attention is also directed to col. 14, line 67 through col. 15, line 1, indicating that it is the user at a network device that signs on the access network and begins the process discussed in Figure 13. The cited section does not disclose Applicants claim limitations of establishing a first set of permissions for the user profile.

Similarly, the Examiners citation of steps 1302, 1304, 1306 and 1308 in Figure 13 as disclosing "establishing a second set of permissions for a selected sub-division of the user profile, wherein said second set of permissions specifies who may access the sub-division" is also misplaced. Step 1302 was discussed above while step 1304 checks to see if the user ID has a provider ID (domain name) embedded in it which may be leveraged to determine where a user profile might be retrieved from using a foreign LDAP interface system (see steps 1306 and 1310). Step 1308 discusses retrieving a default user profile using a local LDAP service in the absence of the domain name being embedded in the user ID. All of these steps relate to servicing a <u>user</u> request and have nothing to do with establishing permissions for different users for fields within a user profile as claimed by Applicants. The cited section thus does not disclose Applicants claim limitations of establishing a first set of permissions for the user profile.

Applicants fourth claimed step in claim 1 includes the limitation of "receiving a request from a non-user party to reference the selected sub-division, the non-user party being an entity other than the user about which the user-profile holds information" based on the first and second set of permissions. As discussed above, Cook does not disclose the establishing of the first and second set of permissions and the requests cited by the Examiner relate to user requests, not those from a non-user party. The Examiner cites step 1312 and components 592 and 572 as disclosing the receipt of the request from the non-user party. As previously noted step 1312 involves a determination as to whether a request from a user is a retrieve request and components 592 and 572 show a user profile.

The cited steps and components do not disclose Applicants' claim element of receiving a request from a non-user party to reference the selected sub-division, the non-user party being an entity other than the user about which the user-profile holds information based on the first and second set of permissions as they only relate to a user request to access their own profile(the user being the subject of the user profile) and do not disclose the use of the first and second set of permissions). Accordingly Applicants request the withdrawal of the rejections directed to claims 1-15.

Similarly for claims 16-19, the Examiner cites Figures 8-11 in general as disclosing the step in independent claim 16 of "granting access permission for authorized information in a selected user profile to a selected one of the groups so that the service providers in the selected group may access the authorized information." However, Figure 8 relates to the creation of a user profile, in response to a user request, using inheritance. Figure 9 discusses the steps followed by the database access system to perform the inheritance and profile creation in response to user selections, see col. 12, lines 36-39). Figures 10 and 11 relate to the execution and updating of a network shell on behalf of the user. The cited figures fail to disclose the claim limitations.

Also for claims 16-19, the Examiner cited components 1414, 1416, 1418 and the subshell in Figure 14 which discusses device, user and service sessions as disclosing the Applicants' claimed step of "transmitting the authorized information to a non-user party in said selected one of the groups in response to a request from the non-user party, the non-user party being an entity other than the user about which the user-profile holds information." The discussion of the cited components of Figure 14 in Cook does not discuss the transmission of authorized information (in a selected user profile) in response to a request from a non-user party. Accordingly Applicants request the withdrawal of the rejections directed to claims 16-19.

The Examiner's rejections for claims 20-25 are also respectfully traversed. The Examiner cited Figure 9, col. 11, line 65- col. 12, line 12 as disclosing Applicants' independent claim 20. Independent claim 20 includes the claim limitations of "providing a preference management server, said preference management server providing access to a user profile, said user profile having various fields of information, wherein at least one of said fields has associated permissions." The cited section in Figure 9 discusses the steps followed by the database access system to perform the inheritance and profile creation in response to user selections. The cited section does not discuss fields of information in a user profile with associated permissions. Accordingly Applicants request the withdrawal of the rejections directed to claims 20-25.

Claims 26-31 were rejected on the same basis as claims 1-25. Applicants respectfully re-assert the above arguments in response. The Examiner also cites Figure 22 which discusses network service authorization. Applicants note that the request being serviced is that of a user accessing the network via a network device, the request is not from a non-user party. Accordingly Applicants request the withdrawal of the rejections directed to claims 26-31.

CONCLUSION

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Applicant believes no fee is due with this statement. However, if a fee is due, please charge our Deposit Account No. 12-0080, under Order No. KAQ-002 from which the undersigned is authorized to draw.

Dated: July 25, 2005

Respectfully submitted,

By John S. Curran
John S. Curran
Registration No.: 50,445
LAHIVE & COCKFIELD, LLP
28 State Street
Boston, Massachusetts 02109
(617) 227-7400
(617) 742-4214 (Fax)
Attorney/Agent For Applicant